REMARKS

This is in response to the Office Action mailed on <u>November 10, 2004</u>, and the references cited therewith.

Claim 17 was amended. Claims 1-20 are now pending in this application.

§*102 Rejection of the Claims*

Claims 1-20 were rejected under 35 USC § 102(e) as being anticipated by Gleichauf et al. (U.S. Patent No. 6,415,321). This rejection is respectfully traversed, at least on the basis that Gleichauf et al. does not show each and every element of the claims. Applicant reserves the right to swear behind the reference at a later date.

Claims 1-3 of the present application refers to the ability to configure security software on a computer network. The elements providing the ability to configure security software include a database engine providing deduction, a network information database, and a security goal database that describes uses that installed hardware and software may support. Further claims reference configuring multiple different types of security software packages based on security goals.

Gleichauf et al. describes a method and system for mapping a network domain. It has an engine that acquires network information and a query engine that responds to queries for network information. Applicant notes that Gleichauf et al. mostly discusses how network information is required. The Office Action cites Col. 5, line 32 through Col. 7 line 10 as anticipating the claims. Gleichauf et al. in the cited columns, at best, allows "network devices to query stored network information from the domain mapping device 46." Col. 5, lines 39-41, and indicates that "intrusion detection system 18 can query engine 52 to obtain network information, such as identification of a device operating system, services and vulnerabilityes, for a network device, such as file server 34, that is protected by intrusion detection system 18. The network information allows intrusion detection system 18 to provide maximum protection of file server 34 or other network devices based upon the most current possible data available through domain mapping device 46. Query engine 52 provides a device configuration for each application running on the network device." Col. 6, lines 50-60.

Note, that claim 1 recites a security goal database. No mention of that type of database is found in Gleichauf et al. As such, a prima facie case of anticipation has not been established, and the rejection should be withdrawn. Further, claim 1 refers to a database engine providing deduction. This element is also not found in Gleichauf et al. A database engine providing deduction. No similar type of active inference ability is described in Gleichauf et al.

Claims 4-9 describe configuring security software packages, and also contains elements that distinguish from Gleichauf et al. in the same manner as claim 1, such as the security goal database. Claim 4 also describes two different types of configuration modules, one for configuring intrusion blocking security software packages, and a second for configuring intrusion detection software packages. Both utilize information regarding the installed configuration and security goals. None of these elements are found in Gleichauf et al. There is reference to an intrusion detection system 18, but no breakdown of it into separate software packages directed to different function is found. Thus, a prima facie case of anticipation has not been established, and the rejection should be withdrawn based on any one of the above missing elements.

The Office Action references Col. 7, lines 10-25 as describing an event database. This language has been reviewed, and appears to be related to "a method for mapping a network domain." Col. 7, lines 10-11. No mention of events, nor an event database is found in the cited language.

Claim 10 distinguishes from Gleichauf et al. for at least the same reasons as claim 4.

Claim 11 distinguishes from Gleichauf et al. in at least the same manner as claim 1. Claim 11 references active inference in a database engine to decompose one or more security policies. The Office Action references Col. 5, lines 15-31 as describing an active inference engine. Such language merely describes the contents of FIG. 2, which is a block diagram depicting a network domain with network devices. There is no reference to any type of active inference database engine.

Regarding claims 12 and 16, the Office Action indicates that Gleichauf et al. discloses "classifying network devices based on an IP address, a network topology and one or more services the individual network device provides, and applying rules to the individual network device based on its classification (Col. 4, lines 47-67 and Col. 5, lines 1-14." Perhaps the most

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.111
Serial Number: 09/943,405
Filing Date: August 30, 2001
Title: AUTOMATED CONFIGURATION OF SECURITY SOFTWARE SUITES

Page 10
Dkt: H0001867

telling information in the cited language is "The stored domain mapping information is available for use by network security devices." Col. 4, lines 66-67. This language appears to indicate that the database merely provides information, and there is no active inference involved. Further, no reference to classification and applying rules is found in the cited langauge.

Claim 15 also references the use of active inference, and the use of one or more security goals in configuring a security software package. As such, it is believed to distinguish the references for at least the same reasons as above.

Claim 17 was amended to correct a typographical error. As in claim 1, an engine using deduction or security goals are not believed to be shown in Gleichauf et al.

Claims 18-20 are also believed to distinguish from Gleichauf et al. for many of the same reasons as described above. Among the differences, claim 18 includes configuring multiple security packages, an engine using deduction, security goals, and configuring multiple security packages using the security goals. It should be noted that Gleichauf et al. does not describe query engine 52 as performing any configuration of the security devices. Rather, it appears that the intrusion detection system 18 uses the query engine to query the database.

Conclusion

Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at (612) 373-6972 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.
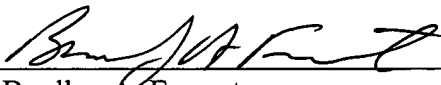
Respectfully submitted,

Robert P. Goldman

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6972

Date ___2-1-2005___   By _____
                              Bradley A. Forrest
                              Reg. No. 30,837

_____Gina M. Uphus_____   _____

Name   Signature